מדריך למשתמש של HP Sure Admin

סיכום

HP Sure Admin מאפשר למנהלי IT לנהל בצורה מאובטחת הגדרות קושחה של התקן רגיש באמצעות אישורים וקריפטוגרפיה של מפתח ציבורי לצורך ניהול מרוחק ומקומי של הגדרות במקום סיסמה.

מידע משפטי

מהדורה שנייה: אוקטובר 2021

מהדורה ראשונה: דצמבר 2019

מק"ט מסמך: L83995-BB2

תוכן העניינים

1 תחילת העבודה

HP Sure Admin מאפשר למנהלי IT לנהל בצורה מאובטחת הגדרות קושחה של התקן רגיש באמצעות אישורים וקריפטוגרפיה של מפתח ציבורי לצורך ניהול מרוחק ומקומי של הגדרות במקום סיסמה.

HP Sure Admin כולל את המרכיבים הבאים:

- **מחשב היעד:** הפלטפורמות לניהול התומכות במצב אימות BIOS משופר.
- **ערכת Manageability Integration Kit (MIK) של HP:** יישום ה-plug-in של System Center Configuration Manager (SCCM) או של תוכנית השירות BIOS Configuration Utility (BCU) של HP לניהול מרחוק של הגדרות ה-BIOS.
- **HP Sure Admin Local Access Authenticator:** אפליקציית טלפון המחליפה את הסיסמה כדי לאפשר גישה מקומית להגדרות ה-BIOS באמצעות סריקת קוד QR כדי לקבל קוד PIN חד-פעמי.

השימוש ב-HP Sure Admin

סעיף זה מתאר את התהליך לשימוש ב-HP Sure Admin.

1. פתח את יישום ה-plug-in של HP Sure Admin בתוך יישום ה-plug-in של HP Manageability Integration Kit (MIK) עבור System Configuration Manager (SCCM) או עבור תוכנית השירות BIOS Configuration Utility (BCU) המשופרת.
2. הורד את אפליקציית הטלפון HP Sure Admin מחנות Google Play™ או מה-App Store® של Apple.
3. צור צמד מפתחות שישמש את התקן היעד ואת אפליקציית הטלפון HP Sure Admin כדי לקבל את קוד ה-PIN החד-פעמי לביטול נעילת ה-BIOS.

השבתת HP Sure Admin

סעיף זה מפרט את האפשרויות להשבתת HP Sure Admin.

- בהגדרות F10 של ה-BIOS, בחר **Restore Security Settings to Factory Defaults** (שחזור הגדרות האבטחה לברירת המחדל של היצרן).

הערה: פעולה זו דורשת נוכחות פיזית לשם הזנת קוד PIN לאימות באמצעות אפליקציית הטלפון HP Sure Admin כדי לגשת להגדרות F10.

- השתמש בפקודת BCU כדי לקרוא מרחוק ל-WMI של **Restore Security Settings to Factory Defaults** (שחזור הגדרות האבטחה לברירת המחדל של היצרן).

הערה: לקבלת מידע נוסף, עיין במדריך למשתמש של תוכנית השירות HP BIOS Configuration Utility (BCU).

- בדף הקצאת האבטחה של MIK, בחר **Deprovision** (ביטול הקצאה).

2 יצירה וניהול של מפתחות

הקצאת אבטחה מלאה מתוך MIK לפני הפעלת מצב אימות BIOS משופר. מצב אימות BIOS משופר חייב להיות פעיל כדי ליצור ולייצא מפתחות. כדי להפעיל את מצב אימות ה-BIOS:

▲ פתח את יישום ה-plug-in של HP Sure Admin ובחר **Enhanced BIOS Authentication Mode** (מצב אימות BIOS משופר) כדי ליצור ולייצא מפתחות.

יצירה וייצוא של מפתחות

ישנן שלוש דרכים שונות ליצור צמדי מפתחות גישה מקומיים ולהפעיל את אפליקציית הטלפון HP Sure Admin כדי לגשת למפתח.

- יצירה וייצוא של מפתחות עם הפצה ידנית בעמוד 2
- יצירה וייצוא של מפתח עם Azure AD Revocation בעמוד 3
- יצירה ושליחה של מפתח אל OneDrive של קבוצת Azure AD: בעמוד 3

יצירה וייצוא של מפתחות עם הפצה ידנית

השתמש באפשרות זו כדי לייצא את מפתח ההרשאה לגישה מקומית ולאחר מכן להפיץ אותו באופן ידני לאפליקציית הטלפון HP Sure Admin בדואר האלקטרוני או בשיטה אחרת.

הערה: אפשרות זו אינה מחייבת גישה לרשת עבור אפליקציית הטלפון HP Sure Admin כדי לקבל קוד PIN חד-פעמי.

1. הענק שם למפתח בתיבת ההזנה **Key Name** (שם מפתח).
2. הזן את ביטוי הסיסמה בתיבת ההזנה **Passphrase** (ביטוי סיסמה).

הערה: ביטוי הסיסמה משמש להגנה על המפתח המיוצא ויש להקצות אותו כדי שמשתמש אפליקציית הטלפון HP Sure Admin יוכל לייבא את המפתח.

3. בחר **Browse** (עיון), ובחר היכן לייצא את הנתיב במערכת.
4. בחר **Create Key** (צור מפתח). המפתח נוצר בהצלחה כאשר מופיע סמל הודעה ליד הלחצן **Create key** (צור מפתח) עם ההודעה **Key successfully created** (המפתח נוצר בהצלחה).
5. בחר את **Next** (הבא). דף הסיכום מציג את הגדרות HP Sure Admin שהזנת.
6. בחר **Save Policy** (שמור מדיניות). המדיניות נשמרה כאשר מופיעה הודעת **Saved successfully** (נשמר בהצלחה).
7. נווט אל התיקייה שבה שמרת את המפתח והפץ אותו למשתמש אפליקציית הטלפון HP Sure Admin בשיטה הזמינה למשתמש זה באותו התקן, כגון דואר אלקטרוני. משתמש זה יזדקק גם לביטוי הסיסמה כדי לייבא את המפתח. HP ממליצה להשתמש במנגנוני הפצה נפרדים עבור המפתח וביטוי הסיסמה.

הערה: בעת שליחת קוד QR, שלח אותו בגודלו המקורי. האפליקציה אינה יכולה לקרוא את התמונה כהלכה אם היא קטנה יותר מגודל של 600 x 800.

יצירה וייצוא של מפתח עם Azure AD Revocation

השתמש באפשרות זו כדי לחבר את מפתח הגישה המקומי לקבוצה מוגדרת של Azure Active Directory ולדרוש מאפליקציית הטלפון HP Sure Admin לחייב את אימות המשתמש עבור Azure Active Directory וכן לאשר שהמשתמש חבר בקבוצה שצוינה לפני מתן קוד PIN לגישה מקומית. שיטה זו מחייבת גם הפצה ידנית של מפתח הרשאת הגישה המקומי לאפליקציית הטלפון בדואר אלקטרוני או בשיטה אחרת.

הערה: אפשרות זו מחייבת את אפליקציית הטלפון HP Sure Admin להיות בעלת גישה לרשת כדי לקבל קוד PIN חד-פעמי.

1. הענק שם למפתח בתיבת ההזנה **Key Name** (שם מפתח).
2. הזן את ביטוי הסיסמה בתיבת ההזנה **Passphrase** (ביטוי סיסמה).

הערה: ביטוי הסיסמה משמש להגנה על המפתח המיוצא ויש להקצות אותו כדי שמשתמש אפליקציית הטלפון HP Sure Admin יוכל לייבא את המפתח.

3. בחר **Azure AD Login** (כניסה אל Azure AD) והתחבר.
4. בחר את שם הקבוצה שלך מהתיבה הנפתחת **Azure AD Group Name** (שם קבוצה של Azure AD). עליך להיות חבר בקבוצה כדי לקבל גישה למפתח.
5. בחר **Browse** (עיון), ובחר היכן לייצא את הנתיב במערכת.
6. בחר **Create Key** (צור מפתח). המפתח נוצר בהצלחה כאשר מופיע סמל הודעה ליד הלחצן **Create key** (צור מפתח) עם ההודעה **Key successfully created** (המפתח נוצר בהצלחה).
7. בחר את **Next** (הבא). דף הסיכום מציג את הגדרות HP Sure Admin שהזנת.
8. בחר **Save Policy** (שמור מדיניות). המדיניות נשמרה כאשר מופיעה הודעת **Saved successfully** (נשמר בהצלחה).
9. נווט אל התיקייה שבה שמרת את המפתח והפץ אותו למשתמש אפליקציית הטלפון HP Sure Admin בשיטה הזמינה למשתמש זה באותו התקן, כגון דואר אלקטרוני. משתמש זה יזדקק גם לביטוי הסיסמה כדי לייבא את המפתח. HP ממליצה להשתמש במנגנוני הפצה נפרדים עבור המפתח וביטוי הסיסמה.

הערה: בעת שליחת קוד QR, שלח אותו בגודלו המקורי. האפליקציה אינה יכולה לקרוא את התמונה כהלכה אם היא קטנה יותר מגודל של 600 x 800.

יצירה ושליחה של מפתח אל OneDrive של קבוצת Azure AD:

(מומלץ) השתמש באפשרות זו כדי להימנע מאחסון של מפתח הרשאת גישה מקומי בטלפון. לאחר בחירה אפשרות זו, MIK יאחסן את מפתח הרשאת הגישה המקומי בתיקיית OneDrive שצוינה, הנגישה רק לקבוצה המורשית. משתמש אפליקציית הטלפון HP Sure Admin יצטרך לבצע אימות ל-Azure AD בכל פעם שיידרש קוד ה-PIN.

1. הענק שם למפתח בתיבת ההזנה **Key Name** (שם מפתח).
2. הזן את ביטוי הסיסמה בתיבת ההזנה **Passphrase** (ביטוי סיסמה).
3. בחר **Azure AD Login** (כניסה אל Azure AD) והתחבר.
4. בחר את שם הקבוצה שלך מהתיבה הנפתחת Azure AD Group Name (שם קבוצה של Azure AD).

הערה: עליך להיות חבר בקבוצה כדי לקבל גישה למפתח.

5. הזן את שם התיקייה של OneDrive שבה ברצונך שהמפתח יישמר בתיבת ההזנה **OneDrive**.
6. בחר **Browse** (עיון), ובחר היכן לייצא את הנתיב במערכת.

7. בחר **Create Key** (צור מפתח).

הערה: המפתח נוסף לתיקיית OneDrive שצוינה ויוצא לתיקייה המקומית שצוינה בהצלחה כאשר מופיע סמל הודעה ליד הלחצן **Create Key** (צור מפתח) עם ההודעה **Key successfully created** (המפתח נוצר בהצלחה).

8. בחר את **Next** (הבא). דף הסיכום מציג את הגדרות HP Sure Admin שהזנת.

9. בחר **Save Policy** (שמור מדיניות). המדיניות נשמרה כאשר מופיעה הודעת **Saved successfully** (נשמר בהצלחה).

הערה: בתרחיש זה, אין צורך לשלוח דבר אל אפליקציית הטלפון HP Sure Admin לשם הקצאה מראש. מחשבי היעד מוקצים כך שהם מצביעים על מיקום OneDrive הכלול בקוד ה-QR. אפליקציית הטלפון HP Sure Admin משתמשת במצביע זה כדי לגשת למיקום OneDrive אם המשתמש הוא חלק מהקבוצה המורשית והוא אומת בהצלחה.

3 הגדרות טלפון

הורד את אפליקציית הטלפון HP Sure Admin מ-Google Play או מ-Apple store.

- הורד את HP Sure Admin מהחנות של Google בטלפונים של Android.
- הורד את HP Sure Admin מהחנות של Apple בטלפונים של iOS.

שימוש באפליקציית הטלפון HP Sure Admin לביטול נעילת ה-BIOS

אפליקציית הטלפון HP Sure Admin מחליפה את השימוש בסיסמת ה-BIOS בגישה מקומית להגדרות ה-BIOS על-ידי מתן קוד PIN חד-פעמי שהתקבל מסריקת קוד ה-QR המוצג על-ידי מחשב היעד.

השתמש בשלבים אלה כדי לשמור את המפתח באופן מקומי בטלפון, בתרחיש שבו המפתח נשלח למשתמש באפליקציית הטלפון. בדוגמה הבאה, המפתח נשלח בדואר אלקטרוני למשתמש באפליקציית הטלפון HP Sure Admin, והמשתמש פותח את הדואר האלקטרוני בטלפון.

1. פתח את הודעת הדואר האלקטרוני המכילה את המפתח.
2. כשמופיע הדף **Enrollment** (הרשמה), הזן את ביטוי הסיסמה בתיבת ההזנה **Enter passphrase** (הזן ביטוי סיסמה) ואת כתובת הדואר האלקטרוני שלך בתיבה **Enter your email address** (הזן את כתובת הדואר האלקטרוני) כדי לפענח את המפתח ולהוסיפו לאפליקציה HP Sure Admin. קוד ה-PIN לביטול הנעילה מוצג בדף **Your PIN** (קוד ה-PIN שלך).

הערה: שלב זה שומר את המפתח בהתקן הנייד ומשלים את ההרשמה. בנקודה זו, באפשרותך להשתמש באפליקציית הטלפון HP Sure Admin כדי לגשת לכל התקן שהוקצה לגישה באמצעות מפתח זה. כתובת דואר אלקטרוני נדרשת רק אם מנהל המערכת מחייב זאת.

3. הזן את קוד ה-PIN בתיבת הקלט **Enter Response Code** (הזן קוד תגובה) של ה-BIOS.

קבלת גישה להגדרת ה-BIOS לאחר הרשמה

כדי לקבל גישה להגדרות ה-BIOS במחשב היעד לאחר ההרשמה:

1. היכנס להגדרות ה-BIOS בעת האתחול במחשב היעד.
2. בחר **Scan QR Code** (סריקת קוד QR) באפליקציית הטלפון וסרוק את קוד ה-QR במחשב היעד.
3. אם תידרש לאימות משתמש, ספק את ההרשאות שלך.
4. קוד ה-PIN לביטול הנעילה מוצג בדף **Your PIN** (קוד ה-PIN שלך).
5. הזן את קוד ה-PIN בתיבת ההזנה **Enter Response Code** (הזן קוד תגובה) של ה-BIOS במחשב היעד.

ביטול נעילה של BIOS באמצעות קבוצת OneDrive של Azure AD

כדי להשתמש ב-HP Sure Admin לביטול נעילת ה-BIOS באמצעות קבוצת OneDrive של Azure AD:

1. בחר **Scan QR Code** (סריקת קוד QR) וסרוק את קוד ה-QR של ה-BIOS.

הערה: אפליקציית HP Sure Admin מציגה את דף הכניסה של Azure AD.

2. היכנס לחשבון Azure שלך.

3. הזן את קוד ה-PIN בתיבת הקלט **Enter Response Code** (הזן קוד תגובה) של ה-BIOS.

הערה: אפליקציית HP Sure Admin לא שומרת את המפתח באופן מקומי בתרחיש זה. אפליקציית הטלפון HP Sure Admin מחייבת גישה לרשת והמשתמש חייב לבצע אימות בכל פעם שיידרש קוד PIN חד-פעמי.

4 קודי שגיאה של HP Sure Admin

השתמש בטבלה בסעיף זה כדי לראות את קודי השגיאה, הסוגים והתיאורים של HP Sure Admin ו-KMS Admin Console.

טבלה 4-1 קודי שגיאה, סוגים ותיאור האפליקציה HP Sure Admin

קוד שגיאה	סוג שגיאה	תיאור
100	QRCodeUnknownError	שגיאה כללית.
101	QRCodeDeserialization	לא ניתן לקרוא את קובץ ה-JSON של קוד ה-QR. המחרוזת אינה קובץ JSON חוקי או שהנתונים לא חוקיים.
102	QRCodeInvalidImage	תמונת קוד QR הסרוקה אינה חוקית. לא ניתן לקרוא את קובץ התמונה של קוד ה-QR.
103	QRCodeNoPayload	תמונת קוד QR הסרוקה אינה חוקית. קובץ התמונה אינו כולל תוכן JSON.
104	QRCodeInvalid	לא ניתן לקרוא את קובץ ה-JSON של קוד ה-QR. המחרוזת אינה קובץ JSON חוקי או שהנתונים בתמונת ה-QR אינם חוקיים.
105	QRCodeInvalidKeyIdHash	קוד ה-Hash של המפתח הציבורי בקובץ JSON של קוד ה-QR אינו תואם לקוד ה-Hash של המפתח הציבורי בחבילת ההרשמה (נתוני KeyID).
106	QRCodeTampered	תמונת קוד QR הסרוקה שונתה ואינה חוקית.
107	QRCodeTamperedOrInvalidPassPhrase	תמונת קוד QR הסרוקה שונתה ואינה חוקית, או שביטוי הסיסמה שהוזן שגויה.

טבלה 4-2 מפתח גישה חד-פעמי משגיאות, סוגים ותיאורים של OneDrive

קוד שגיאה	סוג שגיאה	תיאור
200	OneTimeKeyError	שגיאה כללית.
201	OneTimeKeyNoUserGroups	המשתמש המחובר לא שייך לקבוצת AD כלשהי בארגון.
203	OneTimeKeyInvalidUserGroup	המשתמש המחובר לא שייך לקבוצת ה-AD שמפתח זה הוקצה לה.
204	OneTimeKeyQRFileDoesNotExist	קובץ המפתח החד-פעמי אינו קיים בתיקיית OneDrive של קבוצת ה-AD.
205	OneTimeKeyInvalidQRFile	קובץ המפתח החד-פעמי בתיקיית OneDrive של קבוצת ה-AD אינו חוקי.
206	OneTimeKeyInvalidQRpayload	קובץ המפתח החד-פעמי קיים אך לא ניתן לקרוא את תוכן הקובץ.

טבלה 4-3 שגיאות הרשאה ל-Azure AD

קוד שגיאה	סוג שגיאה	תיאור
300	AzureADUnknownError	שגיאה כללית.
301	AzureADInvalidDomain	כתובת הדואר האלקטרוני שהוזנה אינה תואמת לשם הדומיין בתמונת קוד ה-QR.
302	AzureADAccessToken	אירעה שגיאה בקבלת אסימון גישה מ-Azure AD. המשתמש לא יכול להיכנס ל-Azure AD של הארגון, או שלאפליקציה אין את ההרשאות הנדרשות כדי להתחבר ל-Azure AD של הארגון. ייתכן גם שהמשתמש ביטל את האימות.
303	AzureADUserProfile	אפליקציית HP Sure Admin לא הצליחה לקבל נתוני פרופיל משתמש מ-Azure AD של הארגון.
304	AzureADUserPrincipalMismatch	כתובת הדואר האלקטרוני לא תואמת לשמו העיקרי של המשתמש המחובר.
305	AzureADUserInvalidUserGroup	המשתמש המחובר לא שייך לקבוצת Azure AD שמפתח זה הוקצה לה.

טבלה 4-4 שגיאות, סוגים ותיאורים של KMS Admin Console

קוד שגיאה	סוג שגיאה	תיאור
401	KmsUnauthorized	המשתמש אינו מורשה להשתמש בשירות KMS.
402	KmsKeyDoesNotExist	מפתח פרטי תואם אינו קיים במאגר מפתחות KMS . המפתח נמצא כעת במצב מחיקה אך ניתן לשחזור, ולא ניתן לעשות שימוש חוזר בשם שלו במצב זה. ניתן רק לשחזר או לנקות את המפתח.
403	KmsKeyDoesNotExistInTableStorage	המפתח אינו קיים באחסון טבלה.
404	KmsUploadKeyErrorInKeyVault	אירעה שגיאה בעת הוספת מקש למאגר המפתחות.
405	KmsUploadKeyUnauthorized	המשתמש אינו מורשה להעלות מפתחות. המשתמש אינו שייך לקבוצת AD המורשית שרשאית לקרוא ל-API זה.
406	KmsInvalidAzureADLogin	המשתמש אינו מחובר ל-Azure Tenant AAD.
407	KmsNoUserGroups	המשתמש המחובר אינו שייך לקבוצת AD כלשהי בארגון.
408	KmsInvalidUserGroup	המשתמש המחובר לא שייך לקבוצת ה-AD שמפתח זה הוקצה לה.
409	KmsInvalidAccessToken	אסימון הגישה שסופק בבקשה אינו חוקי.
410	KmsAccessTokenExpired	פג התוקף של אסימון הגישה שסופק.
411	KmsAccessTokenInvalidTenantId	לאסימון הגישה שסופק יש מזהה דייר לא חוקי.
412	KmsAccessTokenTenantIdMismatch	מזהה הדייר באסימון הגישה שסופק אינו תואם למזהה הדייר באפליקציית הפונקציה.
413	KmsInvalidKeyId	מזהה המפתח ריק או Null.
414	KmsDeleteKeyUnauthorized	המשתמש אינו מורשה למחוק מפתחות. המשתמש אינו שייך לקבוצת AD המורשית שרשאית לקרוא ל-API זה.

טבלה 4-4 שגיאות, סוגים ותיאורים של KMS Admin Console (המשך)

קוד שגיאה	סוג שגיאה	תיאור
415	KmsKeyVaultSoftDeleteUnrecoverableState	נכשל הניסיון לשחזר את הסוד, ולא ניתן לשחזר אותו. המשתמש צריך לנסות שוב.
416	KmsInvalidGetKeysRequest	בקשת Get Keys (קבל מפתחות) אינה חוקית.
417	KmsGetKeysUnauthorized	המשתמש אינו מורשה לקבל מפתחות. המשתמש אינו שייך לקבוצת AD המורשית שרשאית לקרוא ל-API זה.
418	KmsInvalidRequestPayload	הבקשה שהתקבלה על-ידי ה-API אינה חוקית.
419	KmsRequestRequired	הבקשה שהתקבלה אינה יכולה להיות ריקה.
420	KmsKeyNotConcurrent	המפתח באחסון הטבלה עודכן או שונה מאז הפעם האחרונה שהמשתמש אחזר עותק.